UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,517	12/11/2003	Gernot Eckstein	I0046.0162	1592

38881 7590 04/12/2011

DICKSTEIN SHAPIRO LLP
1633 Broadway
NEW YORK, NY 10019

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
04/12/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/735,517	**Applicant(s)** ECKSTEIN ET AL.
	Examiner CARLTON V. JOHNSON	**Art Unit** 2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2011*.
2a)☒ This action is **FINAL**. 2b)□ This action is non-final.
3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3 and 5-10* is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)□ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1,3 and 5-10* is/are rejected.
7)□ Claim(s) _____ is/are objected to.
8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.
10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a)□ All b)□ Some * c)□ None of:
1.□ Certified copies of the priority documents have been received.
2.□ Certified copies of the priority documents have been received in Application No. _____.
3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. This action is in response to application amendments filed on 1-25-2011.

2. Claims **1, 3, 5 - 10** are pending. Claims **2, 4** have been cancelled. Claims **1, 3** are independent. This application was filed on 12-11-2003.

Response to Remarks

3. Applicant's arguments have thus been fully considered and they were persuasive, therefore new grounds of rejection have been entered.

3.1 Applicant argues, *varying a supply voltage to time-shift the execution point of operations*.

Kocher discloses that D/A output is provided to a noise production module and that the noise production module is configured to sink power or vary power which also varies the supply voltage. Kocher also discloses that a noise production module may be clocked independently or made to appear to be time-shifted in reference to the execution of other processes. (see Kocher col 5, lines 24-26: D/A output provided to noise production module, which is configured to sink power; col 5, lines 44-47: prevent noise (used to sink or vary power) from being correlated with externally measurable events (operation of processes); multiple noise production modules utilized; col 5, lines 50-60: noise production modules may include delay lines that temporarily isolate their outputs from those of others or they may be clocked independently)

Kocher discloses sinking or varying power (supply voltage) and Kocher also discloses time-shifting the execution of operations. Both events (varying power and time-shifting operation) are produced in correlation to the noise production module.

3.2 Applicant argues, *time varying a supply voltage of an asynchronous circuit using a random number generator*.

The indicated UART is disclosed in the section discussing clock skipping. The sections discussing random noise generation and clock skipping indicate different procedures to complete random noise generation and clock skipping. The section on clock skipping also discusses clock skipping in relation to random noise generation (see Kocher col 7, lines 19-34). Kocher also discloses in Figure 2 (200, 205) that output from the random number generator is input to the clock skipping module. Kocher discuses the random number generator and clock skipping within the same particular section. Different alternatives to implement random number generation and clock skipping are presented. Theses processes (clock skipping and random number generator) indicated within Kocher are not mutually exclusive alternatives.

The UART is disclosed in reference to the implementation of clock skipping with two clocks (an external clock and an internal clock). The UART is used as a buffer between the internal clock region and the I/O interface to ensure it is clocked at the external clock rate. Kocher discloses the implementation of two separate clock signals (external clock and internal clock). Kocher also discloses that this implementation (2 clocks) makes it more difficult for an attacker to locate points of interest if noise is introduced into signal using techniques of present invention. Noise is introduced into the signal using a random number generator. Noise from a random number generator is used to time shift a clock signal. (see Kocher col 7, lines 6-15) the creation of a separate internal clock signal used to control processor timing during cryptographic operation; noise is also introduced into the signal using the techniques of the present invention)

The circuit of Kocher is an asynchronous type circuit. Kocher discloses time varying a supply voltage. Kocher discloses that D/A output is provided to a noise production module which is configured to sink power or vary power (supply voltage). And, Kocher discloses that a noise production module may be clocked independently or made to appear to be time-shifted. (see Kocher col 5, lines 50-60: to drive noise production module faster than or independently from clock rate applied to cryptosystem microprocessor (time shift operations) The noise production module utilizes a random number generator and is configured to sink power or vary power and time shifts operations. (Kocher col 9, lines 3-9: asynchronous receiver/transmitter; col 5, lines 24-26: D/A output provided to noise production module; configured to sink power; col 5, lines 44-56: prevent noise (sink power) from being correlated to clock transitions (time shifting operations))

3.3 Applicant argues, *Independent claim 1.*

Independent claim 3 has similar limitations as independent claim 1. Responses to arguments for independent claim 1 answer arguments against independent claim 3.

3.4 Applicant argues, *Dependent claim 5 -10.*

Arguments against dependent claims are answered by responses to independent claims.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims **1, 3, 5 - 10** are rejected under 35 U.S.C. 102(e) as being anticipated by **Kocher et al.** (US Patent No. **6,327,661**).

With Regards to Claim 1, Kocher discloses a method of preventing the external detection of operations in a digital integrated circuit (see Kocher col 3, line 63 - col 4, line 5: technique of using unpredictable information to protect cryptosystems against external monitoring) comprising an asynchronous circuit (see Kocher col 9, lines 3-9: asynchronous receiver/transmitter) comprising time-varying a supply voltage of said asynchronous circuit, by a random number generator, to time-shift the execution time of operations within said asynchronous circuit; wherein the time variation of said supply voltage takes place in a random way. (see Kocher col 5, lines 22-29: sink power (varying power consumption, supply voltage) to introduce noise; col 4, lines 37-50: randomness source (random number generator) creates noise used to generate unpredictable information)

With Regards to Claim 3, Kocher discloses a digital integrated circuit comprising: an asynchronous circuit (see Kocher col 9, lines 3-9: asynchronous receiver/transmitter), and means for time-varying a supply voltage of said asynchronous circuit to time-shift the execution point of operations within said asynchronous circuit, wherein said means for time-varying said supply voltage comprising a random number generator. (see Kocher col 5, lines 22-29: sink power (varying power consumption, supply voltage) to introduce noise; col 4, lines 37-50: randomness source (random number generator) creates noise used to generate unpredictable information)

With Regards to Claim 5, Kocher discloses the digital integrated circuit according to claim 3, wherein said means for time-varying said supply voltage comprises a noise voltage source driving said random-number generator. (see Kocher col 5, lines 22-29: sink power (varying power consumption, supply voltage) to introduce noise (noise voltage source))

With Regards to Claim 6, Kocher discloses the digital integrated circuit according to claim 3, wherein said means for time-varying said supply voltage further comprises a digital-analog converter transforming the digital values produced by said random-number generator into an analog voltage. (see Kocher col 4, lines 58-67: output converted to digital form using digital/analog converter)

With Regards to Claim 7, Kocher discloses the digital integrated circuit according to claim 3, wherein said means for time-varying said supply voltage further comprises a voltage regulator. (see Kocher col 5, lines 22-29: activation controller enables noise production system, configured to sink power (varying power, regulation of power or voltage))

With Regards to Claim 8, Kocher discloses the digital integrated circuit according to claim 3, wherein said asynchronous circuit is formed for executing a coding algorithm. (see Kocher col 4, lines 37-50: random number generator implemented in software (coding))

With Regards to Claims 9, 10, Kocher discloses the method, digital integrated circuit according to claims 1 and 3, wherein the asynchronous circuit is a type, which performs processing without correlation to a clock. (see Kocher col 6, lines 18-21: clock skipping (clock decorrelation, without correlation to a clock))

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
March 28, 2011

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436